Public Key Infrastructure Implementation (PKI) Plan

The Marine Corps has been a leader in the Department of Defense implementation and management of Public Key Infrastructure (PKI). Since the activation of DoD PKI in 1999, the Marine Corps has aggressively implemented DoD PKI across the Marine Corps Enter-prise Network (MCEN) taking advantage of the security services PKI provides such as non- repudiation, confidentiality, and integrity.

Since DoD PKI's inception the Marine Corps has systematically implemented the infrastructure necessary to successfully meet the DoD PKI requirements. This implementation includes both the issuance of public key certificates to individuals and servers as well as the infrastructure to validate certificates and the repositories of public certificates for individual and network usage. Providing certificates to individuals is accomplished primarily through the issuance of the DoD mandated ID Card, the Common Access Cards (CAC). At this time the Marine Corps has successfully issued more than half-a-million CAC's holding public key certificates for use by individual Marines, government personnel and authorized contractors. Ninety percent of all personnel required possess a CAC.

Public key infrastructure is the framework established to issue, maintain, and revoke public key certificates. The Marine Corps Network Operations Security Com-mand (MCNOSC) is responsible for the operational management and implementation of the DoD PKI within the Marine Corps. The MCNOSC centrally manages PKI as the Registration Authority (RA) for the Marine Corps. The implementation of PKI has been decentralized across the enterprise through a series of Local Registration Authorities (LRA). Both the RA and LRA's form the issuance and revocation infrastructure throughout the Marine Corps. The MCNOSC's RA and LRA infrastructure has remained committed to issuing and revoking server certificates and individual certificates for garrison and operationally deployed units spanning both the unclassified and classified networks. The Marine Corps' PKI implementation also includes an infrastructure to maintain the status of all public key certificates issued within the DoD PKI. The maintenance of certificates includes a public repository of public key encryption certificates and certificate revocation lists as well as an efficient means of validating certificates in use. The MCNOSC has begun installation of a MCEN-wide Online Certifi-cate Status Protocol (OCSP) infrastructure in order to meet the validation requirements of both client machines and network servers across the unclassified and classified networks. The OCSP infrastructure will provide the user a method of validating certificates used to digitally sign e-mails and documents as well as validate certificates for authentication to private web servers and web based application both on the classified and unclassified network. The OCSP infrastructure is a critical element in allowing the Marine Corps to begin using the CAC for logical access to its unclassified network as well as authentication to web based applications.

DoD PKI/CAC will be the backbone for DoD's Identity Management Initiative for use within the Global Information Grid. The Marine Corps remains firmly committed to PKI implementation and enabling applications to take full advantage of the security services that PKI provides. The Marine Corps continues to lean forward in supporting the DoD's PKI requirements for specific programs and remains flexible to meet mission needs as they arise.